Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1-32 (canceled).

Claim 33 (currently amended) A computer-readable medium having computer-executable instructions for performing a process to prevent digital intrusions, the process comprising:

(a) detecting a request for access by a second computer of a digital tracking component residing on a first computer;

(b) automatically determining if the second computer is associated with the digital tracking component that is being requested by the second computer; ~~and~~

(c) in response to determining that the second computer is associated with the digital tracking component, automatically allowing the second computer to access the digital tracking component;

(d) comparing a domain name of the second computer with a domain name associated with the digital tracking component;

(e) in response to a match of the domain names, determining that the second computer is associated with the digital tracking component; and

(f) in response to a mis-match of the domain names, determining that the second computer is not associated with the digital tracking component, wherein a browser operating within the first computer performs steps (a) through (f).

Claim 34 (canceled).

Claim 35 (previously presented) The medium of claim 33 further comprising:

in response to determining that the second computer is not associated with the digital tracking component, alerting a user of the first computer; and

optionally allowing or preventing access to the digital tracking component by the second computer.

Claim 36 (previously presented) The medium of claim 33 further comprising:

in response to determining that the second computer is not associated with the digital tracking component, automatically blocking the second computer from accessing the digital tracking component.

Claim 37-38 (canceled).

Claim 39 (previously presented) The medium of claim 33, wherein the first computer is a remote client and the second computer is a host server.

Claim 40 (previously presented) The medium of claim 33, wherein steps (a) through (c) occur without intervention from a user of the first computer.

Claim 41 (previously presented) The medium of claim 33, wherein digital communication between the first and second computers occurs on a networked connection comprising a World Wide Web Internet connection.

Claim 42 (previously presented) The medium of claim 33, wherein the digital tracking component is a cookie.

Claim 43 (previously presented) The medium of claim ~~34~~ 33, further comprising:

in response to a match of the domain names, determining that the second computer previously created the digital tracking component residing on the first computer; and

in response to a mis-match of the domain names, determining that the digital tracking component residing on the first computer was created by a third computer.

Claim 44 (previously presented) The medium of claim 35, wherein the alerting step comprises at least one of sounding an audible alert or displaying a color coded visual alert on the first computer.

Claim 45 (currently amended) A computer-implemented method for protecting a first computer from digital intrusions by a second computer, the method comprising:

(a) sending by the second computer to the first computer a request for access of a digital tracking component residing on the first computer;

(b) if the second computer is associated with the digital tracking component that is being requested, the second computer automatically receiving access to the digital tracking component by the first computer; ~~and~~

(c) if the second computer is not associated with the digital tracking component, the second computer automatically being denied access to the digital tracking component by the first computer;

(d) comparing a domain name of the second computer with a domain name associated with the digital tracking component;

(e) in response to a match of the domain names, determining that the second computer is associated with the digital tracking component; and

(f) in response to a mis-match of the domain names, automatically determining that the second computer is not associated with the digital tracking component, wherein steps (a) through (f) are performed by a browser operating within the first computer.

Claim 46 (previously presented) The computer-implemented method of claim 45, wherein determining if the second computer is associated with the digital tracking component comprises comparing a domain name of the second computer with a domain name associated with the digital tracking component.

Claim 47 (previously presented) The computer-implemented method of claim 45, wherein if the second computer is not associated with the digital tracking component, a user of the first computer is alerted.

Claim 48 (previously presented) The computer-implemented method of claim 47, wherein after the user of the first computer is alerted, the first user is given an option to allow or prevent access of the digital tracking component by the second computer.

Claim 49 (previously presented) The computer-implemented method of claim 47, wherein the alert includes at least one of sounding an audible alert or displaying a color coded visual alert on the first computer.

Claim 50 (currently amended) A computer-implemented method for protecting a first computer from digital intrusions by a second computer, comprising:

(a) detecting a request for access by the second computer of a digital tracking component residing on the first computer;

(b) automatically determining if the second computer is associated with the digital tracking component that is being requested by the second computer; ~~and~~

(c) in response to determining that the second computer is associated with the digital tracking component, automatically allowing the second computer to access the digital tracking component;

(d) comparing a domain name of the second computer with a domain name associated with the digital tracking component;

(e) in response to a match of the domain names, determining that the second computer is associated with the digital tracking component; and

(f) in response to a mis-match of the domain names, automatically determining that

the second computer is not associated with the digital tracking component, wherein steps (a) through (f) are performed by a browser operating within the first computer.

Claim 51 (canceled).

Claim 52 (previously presented) The method of claim 50 further comprising:

in response to determining that the second computer is not associated with the digital tracking component, alerting a user of the first computer; and

optionally allowing or preventing access to the digital tracking component by the second computer.

Claim 53 (canceled).

Claim 54 (canceled).

Claim 55 (previously presented) The method of claim 50, wherein the first computer is a remote client and the second computer is a host server.

Claim 56 (previously presented) The method of claim 50, wherein steps (a) through (c) occur without intervention from a user of the first computer.

Claim 57 (previously presented) The method of claim 50, wherein digital communication between the first and second computers occurs on a networked connection comprising a World Wide Web Internet connection.

Claim 58 (previously presented) The method of claim 50, wherein the digital tracking component is a cookie.

Claim 59 (previously presented) The method of claim ~~51~~ 50, further comprising:

in response to a match of the domain names, determining that the second computer previously created the digital tracking component that resides on the first computer; and

in response to a mis-match of the domain names, determining that the digital tracking component residing on the first computer was previously created by a third computer.

MH 6/9/05

Claim 60 (previously presented) The method of claim 52, wherein the alerting step comprises sounding an audible alert or displaying a color coded visual alert on the first computer.

Claim 61 (previously presented) The method of claim 50, further comprising:

in response to determining that the second computer is not associated with the digital tracking component, automatically blocking the second computer from accessing the digital tracking component.

Claim 62 (previously presented) A computer security system for preventing host servers from taking inappropriate self-contained packets of information residing on a remote client, the system comprising:

a monitor module that monitors requests for access by the host servers of the self-contained packets of information residing on a remote client during digital communication between the remote client and the host server; ~~and~~

a notify module that sends an alert to the remote client if a domain name associated with a particular host server does not match a domain name associated with one of the self-contained packets of information residing on a remote client that is being requested by the particular host server;

a compare module that compares a domain name of the host server with a domain name associated with the self-contained packet;

wherein the compare module, ~~(e)~~ in response to a match of the domain names, ~~determining~~ determines that the host server is associated with the self-contained packet; ~~and~~

MH 8/9/05

wherein the monitor module, ~~(f)~~ in response to a mis-match of the domain names, automatically ~~determining~~ determines that the host server is not associated with the digital tracking component and wherein ~~steps (a) through (f) are performed by~~ a browser operating within the remote ~~computer~~ client. MEH, 8/9/05

the monitor module and the compare module are within

Claim 63 (previously presented) The computer security system of claim 62, wherein the notify module provides an audible notification to the remote client when a particular host server requests one or more of the self-contained packets of information that contains information that is not associated with the particular host server.

Claim 64 (previously presented) The computer security system of claim 62, wherein the monitor module uses a color coded visual alert represented by a graphical display that displays a safe color when one of the host servers requests one or more of the digital tracking components that contains information that is associated with the host server and a warning color when one of the host servers requests one or more of the digital tracking components that contains information that is not associated with the host server.